A Comparative Study on Secured Image Transmission Using Steganography Techniques

R. BharathiPriya
M.Phil Research Scholar, PG & Research Department of Computer Science,
Government Arts College, Udumalpet, Tamil Nadu, India.
Email: bharathipriya1292@gmail.com
Dr. E. Karthikeyan
Head of the Department, Assistant Professor, PG & Research Department of Computer Science,
Government Arts College, Udumalpet, Tamil Nadu, India.
Email: e_karthi@yahoo.com

----------**ABSTRACT**----------
Due to the advancements in latest network technology, security of data transformation is a big problem in this society. The need for a secure data handling method for the transmission and storage of text and digital media, comprising patient's diagnostic history, imaging, scans, etc., are indispensable. To secure above mentioned data, steganography plays a vital role in network communication. Steganography means hiding a secret message (the embedded message) within a larger one (source cover) in such a way that an observer cannot detect the presence of contents of the hidden message. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of Steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the Steganography technique used. This paper intends to give an overview of image Steganography, its uses and techniques. It also attempts to identify the requirements of a good Steganography algorithm and briefly reflects on which Steganography techniques are more suitable for which applications.

Keywords - Cover writing, Frequency Domain, LSB method, Spatial domain, Steganography.

----

1. INTRODUCTION

Since the rise of the Internet one of the most important Factors in networking is the security of information. Steganography is the art and science of invisible communication. It is accomplished by hiding information in other information, thus hiding the existence of the information. Steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing"[1] defining it as "covered writing". In the image Steganography the information is hidden exclusively in images. The idea and practice of information hiding has a long past. In Histories the Greek historian Herodotus writes of a Nobleman, Histaeus, who needs to communicate with his son-in-law in Greece, has shaved the head of one of most trusted slave and tattooed the message onto the slave's scalp. When the slave's hair grew back he sends slave with the hidden message and when slave reaches to the destination again he shaved his scalp and retrieve the message [2]. In the Second World War the Germans introduces new data hiding technique which is known as Microdot technique.

In this the information, like photographs, was reduced in size until it was the size of a typed period. It was extremely difficult to detect hidden information, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [3]. Today Steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Although related to cryptography, they are not similar. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message in such a way that it cannot be understood. Steganography and cryptography are techniques used to protect information from unwanted parties but neither technology alone is perfect. Once the presence of hidden information is revealed or suspected, the reason of Steganography is partly defeated. The strength of Steganography increases by combining it with cryptography.

The Steganography has been categorized into (i) Spatial domain Steganography: It mainly includes LSB Steganography and Bit Plane Complexity Slicing (BPS) algorithm. Spatial domain is frequently used because of high capability of hidden information and easy realization. (ii) Transform domain Steganography: The secret information is embedded in the transform coefficients of the cover image. Examples of transform domain Steganography are Discrete Cosine Transform, Discrete Fourier Transform and Discrete Wavelet Transform.

Steganography used for wide range of applications such as defiance organizations for safe circulation of secret data,

intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials, medical imaging where patient's details are embedded within image providing protection of information and reducing transmission time.

2. PRINCIPLE OF STEGANOGRAPHY

The secret message is embedded inside the cover object in encrypted format by using a hiding algorithm and it sent to a receiver over a network. The receiver then decrypted the message by applying the reverse process on the cover data and reveals the secret data [4].

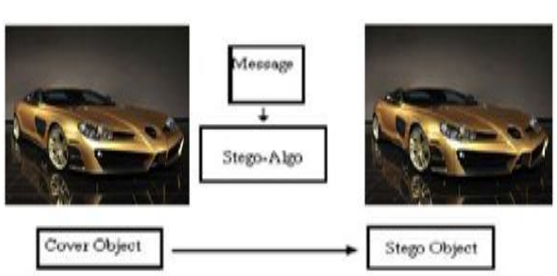

Fig. 1: The principle of Steganography

Fig. 1 shows the principle of Steganography. Steganography algorithm, tries to preserve the perceptive properties of the original image. A suitable image, called as cover/ carrier, is chosen. The secret message is then embedded into the cover using the Steganography algorithm, in a way that does not change the original image in a human noticeable way. The result is new image, the stego-image, which is not looks different than original image.

3. TYPES OF STEGANOGRAPHY

Steganography can used for almost all digital file formats, but the formats those are with a high degree of redundancy are more suitable. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [4]. Image and audio files especially comply with this necessity, while research has also uncovered other file formats that can be used for information hiding. There are four categories of file formats that can be used for Steganography shown in fig. 2.

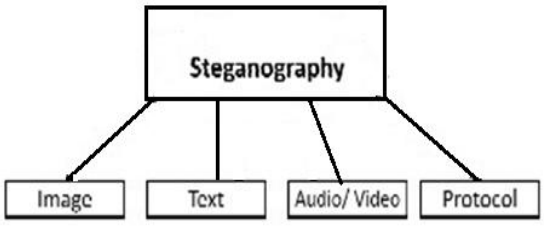

Fig. 2: Types of Steganography

Since, images are quite popular cover or carrier objects used for Steganography. In the domain of digital images different image file formats exist, most of them are available for specific applications.

4. IMAGE STEGANOGRAPHY

The basic model for Steganography is shown on fig. 3. It shows the basic process involved in Steganography which consists of Carrier, Message and Key. Carrier is also known as cover-object, in which message is embedded and serves to hide the presence of the message. The data can be any type of data (plain text, cipher text or other image) that the sender wishes to remain confidential. Key is known as stego-key, which ensures that only recipient who knows the key, corresponding decoding key will be able to recover the message from a cover-object. The cover-object with the object secretly embedded message is then called the stego-object [4].

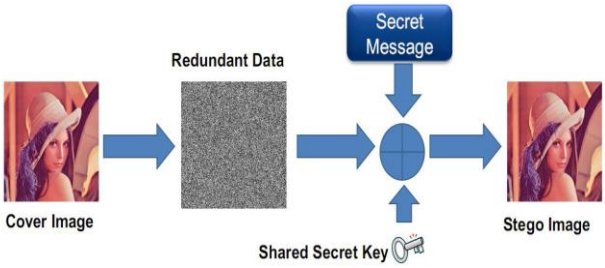

Fig. 3: Basic Steganography Model

Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a object stego-key was used during the information encoding process.

5. IMAGE STEGANOGRAPHY TECHNIQUES

Steganography in images are classified into two categories: Spatial-domain based Steganography and the Transform domain based Steganography.

5.1. SPATIAL DOMAIN METHOD

In spatial domain scheme, the secret messages are embedded directly. In this, the most common and simplest Steganography method is the least significant bits (LSB) insertion method. In LSB technique, least significant bits of the pixels are replaced by the message bits which are permuted before embedding [5].

5.1.1 Least Significant Bit Technique

Least significant bit (LSB) Replacement is a common, simple approach to embedding information in a cover image. The least significant bit (8 bit) of some or all of the bytes inside an image is replaced with a bit of the hidden message. When using a 24-bit image, a bit of each of the red, green and blue color can be used, since they are each represented by a byte. That is one can store 3 bits in each pixel. The image of 800 X 600 pixel, can thus store a total

amount of 1,440,000 bits or 180,000 bytes of embedded data [6].

For example, 3 pixels grid for of a 24-bit image can be as follows:
(00101101 00011100 11011101)
(10100111 11000101 00001101)
(11010010 10101101 01100011)
When the number 500, which binary representation is 11110100, is embedded into the least significant bits of this part of the image. The resulting grid is as follows:
(00101101 0001110**1** 11011101)
(10100111 1100010**0** 00001101)
(11010010 1010110**0** 01100011)

Above the number was embedded into the first 8 bytes of the grid, from these only the 3 underlined bits needed to be changed according to the message which is embedded. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are possible intensities of each primary color is 256, By changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be identify by the human eye, thus the message is successfully hidden in image.

Fig. 4: (a) The cover image (b) The cover image

5.1.2 HIDING GRAY IMAGES USING BLOCKS TECHNIQUE

Internets are becoming popular, channels for communication the security of digital media becomes greater issue. The hiding of a message will reduce the possibility of detecting the secret message. This method allows to hides gray image in one another. In this method the cover is divided into blocks of equal sizes, Each block size is same as that size of the embedding image [4].
Compare each pixel in embedding image with all the corresponding pixels in the blocks of the cover image i.e. pixel (i,j) in the embedding image is compared with the pixel (i,j) in all C blocks of cover image. Select the best pixel to embed. Embed has a value 254, and corresponding pixels values are: 248, 230, 249, 252, 255,260, 270, and 262 (assume cover is divided into 8 blocks). Then the pixel with value 255 will be selected to embed 254.

5.2 TRANSFORM DOMAIN METHOD

The transform domain Steganography technique is used for hiding a large amount of data and provides high security, a good invisibility and no loss of secret message. The goal behind that is to hide information in frequency domain by altering magnitude of all of discrete cosine transform (DCT) coefficients of cover image. The 2-D DCT converts image blocks from spatial domain to frequency domain. The cover image is divided into non overlapping blocks of size 8×8 and applies DCT on each of blocks of cover image using forward DCT [7].

5.2.1 JPEG IMAGE STEGANOGRAPHY TECHNIQUE

Originally it was thought that Steganography would not be possible to use with JPEG images, since they use lossy compression which results in parts of the image data being altered. One of the key characteristics of Steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be damaged. Even if one could somehow keep the message intact it would be difficult to embed the message without the changes being noticeable because of the harsh compression applied. Still, properties of the compression algorithm have been exploited in order to develop a steganographic algorithm for JPEGs [6].

One of these properties of JPEG is exploited to make the changes to the image unseen to the human eye. During the DCT transformation phase of the compression algorithm, rounding errors occur in the coefficient data that are not noticeable and understandable. Although this property is what classifies the algorithm as being lossy, this property can also be used to hide messages. It is neither feasible nor possible to embed information in an image that uses lossy compression, since the compression would destroy all information in the process. So, it is important to recognize that the JPEG compression algorithm is actually divided into lossy and lossless stages. The quantization and the DCT phase form part of the lossy stage, whereas the Huffman encoding used to further compress the data is lossless.

Steganography can take place between these two stages. Using the same principles of LSB insertion the message can be embedded into the least significant bits of the coefficients before applying the Huffman encoding. By embedding the information at this stage, in the transform domain, it is extremely hard to detect, since it is not in the visual domain.

5.2.2 SPREAD SPECTRUM IMAGE STEGANOGRAPHY TECHNIQUE

The Spread Spectrum Image Steganography (SSIS) of the present invention is a data hiding/secret communication steganographic system which uses digital imagery as a cover signal. Spread spectrum provides the ability to hide a significant quantity of information bits within digital images while avoiding detection by an observer. The message is recovered with lowest error probability due the use of error control coding. Spread spectrum image steganography payload is, at a minimum, an order of magnitude greater than of existing watermarking techniques. Furthermore, the original image is not needed to extract the hidden message. The proposed receiver need only possess a key in order to reveal the secret message. The existence of the hidden

information is virtually undetectable by human or computer analysis. At last, SSIS provides resiliency to transmission noise, like which found in a wireless environment and low levels of compression.

	Invisibility	Payload capacity	Robustness against statistical attack	Robustness against image manipulation	Independent of file format	Unsuspicious files
LSB in BMP	High	High	Low	Low	Low	Low
LSB in GIF	Medium	Medium	Low	Low	Low	Low
JPEG	High	Medium	Medium	Medium	Low	High
Spread Spectrum	High	Medium	High	Medium	High	High

6. EVALUATION

The most important requirement is that a Steganographic algorithm has to be imperceptible. Below criteria has been proposed for imperceptibility of an algorithm:

Table 1: Comparison of image Steganography techniques

1) Invisibility- The invisibility of a Steganographic algorithm is most important requirement. Strength of Steganography lies in its ability to be unnoticed by human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised [8].

2) Payload capacity- Watermarking, needs to embed only a small amount of copyright information, In other hand Steganography requires sufficient embedding capacity [9].

3) Robustness against statistical attacks- Statistical Steganalysis is the practice of detecting hidden information by applying statistical tests on image data. Many Steganographic algorithms leave a "signature" when embedding information that can be easily detected through statistical analysis.

4) Robustness against image manipulation- While being transmitted the image may undergo changes by an active attacker in an attempt to remove hidden Information. Image manipulation, such as cropping or rotating, can be performed on the image. This may destroy the hidden message. It is required for Steganographic algorithms to be robust against malicious changes to the image.

5) Independent of file format- The most powerful Steganographic algorithms thus possess the ability to embed information in any type of file.

6) Unsuspicious files- This requirement includes all characteristics of a Steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

7. CONCLUSION

The main image steganographic techniques were discussed in this paper, there exists a large selection of approaches to hiding information in images. Different image file formats have different methods of hiding messages, that having different strong and weak points respectively. Whereas one technique lacks in payload capacity, while other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but it can hides only a very small amount of information. The Least significant bit (LSB) technique in both BMP and GIF makes up for this, but these both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. For an agent to decide on which steganographic algorithm to use, first to decide on the type of application then to use the algorithm and if willing to compromise on some features to ensure the security of others.

REFERENCES

[1] T. Sharp, "An implementation of key-based digital signal Steganography", in Proc. Information Hiding Workshop, Springer LNCS 2137, pp. 13–26, 2001.

[2] Jarno Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume : 13, Issue : 5, pp. 285- 287.

[3] K..M. Singh, L.S. Singh, A.B. Singh and K.S.Devi, "Hiding Secret Message in Edges of the Images", Information and Communication Technology, 2007. ICICT '07, pp. 238 -241.

[4] Jagvinder Kaur and Sanjeev Kumar," Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011.

[5] Johnson, N.F and Jajodia, S., "Exploring Steganography:Seeing the Unseen", Computer Journal, February 2008.

[6] Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355 - 372.

[7] Blossom kaur1, Amandeep kaur2 and Jasdeep singh,"Steganographic approach for hiding image in dct domain" International Journal of Advances in Engineering & Technology, July 2011.

[8] R.Amirtharajan and R.Akila," A Comparative Analysisof Image Steganography;" International Journal of ComputerApplications (0975 – 8887) ,Volume 2 – No.3, May 2010.

[9] V. Nagaraj, Dr. V. Vijayalakshmi and Dr. G. Zayaraz, "Modulo based Image Steganography Technique against Statistical and Histogram Analysis", IJCA Special Issue on"Network Security and Cryptography" NSC, 2011.